

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

L Number	Hits	Search Text	DB	Time stamp
1	4	((("5502764") or ("5414772") or ("5625695") or ("5910989")).PN.	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/18 07:52
3	1	"02086"	EPO; DERWENT; IBM_TDB	2004/08/18 08:06
4	0	"commercialization of dual signatures"	EPO; DERWENT; IBM_TDB	2004/08/18 08:06
5	3	"dual signatures"	EPO; DERWENT; IBM_TDB	2004/08/18 08:08
6	24	"dual signatures"	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/18 08:12
7	33	"double signatures"	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/18 08:19
8	2	"twin signatures"	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/18 08:53
9	19	((doubl\$2 dual\$2) adj signed)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/18 08:58
10	30	redundan\$4 adj signature	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/18 08:58

L Number	Hits	Search Text	DB	Time stamp
10	30	redundan\$4 adj signature	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/18 09:35
11	11351	video and signature	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/18 09:36
15	26	380/202.ccls. and signature and public	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/18 09:46
16	0	(380/202.ccls. and signature and public) and 380/30.ccls.	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/18 09:46
20	33	380/202.ccls. and signature	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/18 09:47
21	0	380/202.ccls. and 380/30.ccls.	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/18 09:48
22	1	380/202.ccls. and 380/31.ccls.	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/18 09:48

L Number	Hits	Search Text	DB	Time stamp
23	6	probabilistic adj signature	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/18 10:01
24	22	("same" with signature) and multicasting	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/18 10:01

09802968

Michael J. Simitoski

Michael.Simitoski@uspto.gov

(703) 305-8191

Google

"chopping function" digital signature

"chopping function" signature

naccache dsa signature

dsa without hash

hashless dsa

(hashless OR hash OR "hash-free") dsa without signature

"more than one signature" digital signature

redundant signatures

"twin signatures"

twinning (digital signatures)

sign same message twice "digital signature"

ACM

+author:naccache

+"digital signature" "twinning" "dual signatures" "double signatures" "twin signatures"

IEEE

("dual signatures" <or> "twinning" <or> "twin signatures")

(dual signatures <or> twinning <or> twin signatures) <and> ('digital signatures' <or> 'digital signature')

Other

Search tool

INSPEC

Search Terms

twin adj signatures

dual adj signatures

double adj signatures

Applications/Patents from Inventor Search

09/308,369

10/130,937

10/048,216

Dialog DataStar[options](#)[logout](#)[feedback](#)[help](#)[databases](#)[search](#)
[page](#)

Titles

To view one or many selected titles scroll down the list and click the corresponding boxes. Then click display at the bottom of the page. To view one particular document click the link above the title to display immediately.

Documents 1 to 1 of 1 from your search "**dual ADJ signatures**" in all the available information:
Number of titles selected from other pages: 0

☐ ¹ [display full document](#)

1998. (INZZ) SET protocol for Visa and Eurocard/Mastercard transactions over the Internet.

Selection	Display Format	Display in	ERA SM Electronic Redistribution & Archiving
<input checked="" type="radio"/> from this page <input type="radio"/> from all pages	<input checked="" type="radio"/> Full <input type="radio"/> Free <input type="radio"/> Short <input type="radio"/> Medium <input type="radio"/> Custom Help with Formats	<input checked="" type="radio"/> HTML <input type="radio"/> Tagged (for tables)	Copies you will redistribute: <input type="text"/> Employees who will access archived record (s): <input type="text"/> Help with ERA
Sort your entire search result by <input type="text" value="Publication year"/> <input type="button" value="v"/> <input type="text" value="Ascending"/>			

[Top](#) - [News & FAQs](#) - [Dialog](#)

© 2004 Dialog

Dialog DataStar[options](#)[logout](#)[feedback](#)[help](#)[databases](#)[search page](#)

Titles

To view one or many selected titles scroll down the list and click the corresponding boxes. Then click display at the bottom of the page. To view one particular document click the link above the title to display immediately.

Documents 1 to 1 of 1 from your search "**twin ADJ signatures**" in all the available information:
 Number of titles selected from other pages: 0

☐ 1 [display full document](#)

1996. (INZZ) Global to microscale evolution of the Pinatubo volcanic aerosol derived from diverse measurements and analyses.

Selection	Display Format	Display in	ERA SM Electronic Redistribution & Archiving
<input checked="" type="radio"/> from this page <input type="radio"/> from all pages	<input checked="" type="radio"/> Full <input type="radio"/> Free <input type="radio"/> Short <input type="radio"/> Medium <input type="radio"/> Custom Help with Formats	<input checked="" type="radio"/> HTML <input type="radio"/> Tagged (for tables)	Copies you will redistribute: <input type="text"/> Employees who will access archived record (s): <input type="text"/> Help with ERA
<div>Sort your entire search result by <input type="text" value="Publication year"/> <input type="text" value="Ascending"/></div>			

[Top](#) - [News & FAQs](#) - [Dialog](#)

© 2004 Dialog

Dialog DataStar[options](#)[logoff](#)[feedback](#)[help](#)[databases](#)[search page](#)

Titles

To view one or many selected titles scroll down the list and click the corresponding boxes. Then click display at the bottom page. To view one particular document click the link above the title to display immediately.

Documents 1 to 2 of 2 from your search "**double ADJ signatures**" in all the available information:
Number of titles selected from other pages: 0

☐ **Select All**

☐ 1 [display full document](#)

2002. (INZZ) Fair electronic cash based on **double signatures**.

☐ 2 [display full document](#)

1997. (INZZ) Dual representations of GL/sub infinity / and decomposition of Fock spaces.

Selection	Display Format	Display in	ERA SM Electronic Redistribution & Archiving
<input checked="" type="radio"/> from this page <input type="radio"/> from all pages	<input checked="" type="radio"/> Full <input type="radio"/> Free <input type="radio"/> Short <input type="radio"/> Medium <input type="radio"/> Custom Help with Formats	<input checked="" type="radio"/> HTML <input type="radio"/> Tagged (for tables)	Copies you will redistribute: <input type="text"/> Employees who will access archived record (s): <input type="text"/> Help with ERA
<div>Sort your entire search result by <input type="text" value="Publication year"/> <input type="text" value="Ascending"/></div>			

[Top](#) - [News & FAQs](#) - [Dialog](#)

© 2004 Dialog

SET protocol for Visa and Eurocard/Mastercard transactions over the Internet.

Accession number & update

5896237, C9806-6130S-004; 980428.

Author(s)

Willems-J.

Source

Elektronik (Germany), vol.47, no.2, p.72-4, 76-8, 20 Jan. 1998. , Published: Franzis-Verlag.

CODEN

EKRKAR.

ISSN

ISSN: 0013-5658.

Availability

SICI: 0013-5658(19980120)47:2L:72:PVEM; 1-3.

Publication year

1998.

Language

GE.

Publication type

J Journal Paper.

Treatment codes

A Application; P Practical.

Abstract

The SET (Secure Electronic Transaction) protocol is announced, which is to allow secure commerce and payments over the Internet. It is stated that Mastercard and Visa are to employ this system. Demonstration screens for order and payment entry are included and a purchasing sequence with SET is explained in detail.

Dual signatures are to be employed to achieve data protection. (0 refs).

Descriptors

access-control; access-protocols; debit-transactions; EFTS; Internet; MasterCard; purchasing;
security-of-data; Visa.

Keywords

SET protocol; Visa transactions; Eurocard transactions; Mastercard transactions; Internet; secure electronic transaction protocol; secure commerce; secure payments; ***dual signatures***; data protection.

Classification codes

C6130S (Data security).
C5640 (Protocols).
C7120 (Financial computing).

Copyright statement

Copyright 1998, IEE.

COPYRIGHT BY Inst. of Electrical Engineers, Stevenage, UK

Fair electronic cash based on *double signatures*.

Accession number & update

7559377, C2003-04-7120-030; 20030324.

Author(s)

Chen-Xiaofeng; Wang-Changjie; Wang-Yumin.

Author affiliation

Nat Key Lab of ISN, Xidian Univ, Xi'an, China.

Source

Journal-of-Computer-Science-and-Technology (English Language Edition) (China), vol.17, no.6, p.830-5, Nov. 2002. , Published: Science Press.

CODEN

JCTEEM.

ISSN

ISSN: 1000-9000.

Availability

SICI: 1000-9000(200211)17:6L.830:FECB; 1-M.

Publication year

2002.

Language

EN.

Publication type

J Journal Paper.

Treatment codes

A Application; P Practical.

Abstract

In order to decrease crimes such as money laundering, blackmailing etc. in electronic cash systems, fair electronic cash has been a major focus of academic research in electronic commerce. When a bank finds some dubious cash or owner, the trusted entity or trustee can help him to revoke the anonymity of the cash. In the previous protocols, the trustee knows all the information of the cash whether he is trusted or not, that is, he can trace the user or cash unconditionally. Furthermore, the dishonest trustee may deceive a user, which means that he may withdraw cash while tracing other users. Such cases are unfair to the honest users. A new fair electronic cash protocol based on untrustworthy trustees is proposed in this paper. The key idea is that the coin structure should include the *signatures* of both the trustee and the bank so that the trustee shares the information of the cash with the bank, while we do not use the secret sharing scheme. In contrast with the previous protocols, neither the trustee nor the bank can trace the money without the help of the other entity. In this way, the privacy of the user is protected furthest. Also, the trustee is off-line in the protocol, which means that he will not be involved in withdrawing the cash. Therefore, the protocol is efficient for implementation. (16 refs).

Descriptors

electronic-money; message-authentication; protocols.

Keywords

fair electronic cash; *double signatures*; crimes; money laundering; data privacy; blackmailing; electronic commerce; protocols.

Classification codes

C7120 (Financial computing).
C6130S (Data security).
C5640 (Protocols).

Copyright statement

Copyright 2003, IEE.

File 8: Ei Compendex(R) 1970-2004/Aug W2
(c) 2004 Elsevier Eng. Info. Inc.
File 35: Dissertation Abs Online 1861-2004/May
(c) 2004 ProQuest Info&Learning
File 65: Inside Conferences 1993-2004/Aug W2
(c) 2004 BLDSC all rts. reserv.
File 2: INSPEC 1969-2004/Aug W2
(c) 2004 Institution of Electrical Engineers
File 94: JICST-EPlus 1985-2004/Jul W4
(c) 2004 Japan Science and Tech Corp(JST)
File 6: NTIS 1964-2004/Aug W3
(c) 2004 NTIS, Intl Cpyrght All Rights Res
File 144: Pascal 1973-2004/Aug W2
(c) 2004 INIST/CNRS
File 434: SciSearch(R) Cited Ref Sci 1974-1989/Dec
(c) 1998 Inst for Sci Info
File 34: SciSearch(R) Cited Ref Sci 1990-2004/Aug W2
(c) 2004 Inst for Sci Info
File 99: Wilson Appl. Sci & Tech Abs 1983-2004/Jul
(c) 2004 The HW Wilson Co.
File 266: FEDRIP 2004/Jun
Comp & dist by NTIS, Intl Copyright All Rights Res
File 95: TEME-Technology & Management 1989-2004/Jun W1
(c) 2004 FIZ TECHNIK
File 62: SPIN(R) 1975-2004/Jun W3
(c) 2004 American Institute of Physics
File 239: Mathsci 1940-2004/Oct
(c) 2004 American Mathematical Society

Set	Items	Description
S1	16812	(ELECTRONIC? OR DIGITAL?) (2N) (SIGNATURE? ? OR SIGN? ? OR S- IGNED OR SIGNING) OR DSA
S2	352	(WITHOUT OR NO OR "NOT" OR T) (5W) HASH??? OR HASHLESS OR UN- HASHED
S3	4513	SIGN??? (5W) (TWICE OR (TWO OR 2ND OR SECOND OR ANOTHER OR E- XTRA OR ADDITIONAL) (1W) TIME? ? OR MORE() (THEN OR THAN) OR AGA- IN OR ONCE() MORE)
S4	3502	(MULTIPLE OR MULTIPLICITY OR SEVERAL OR MORE() (THEN OR THA- N) () ONE OR MANY OR PLURAL? OR DUAL? OR ANOTHER OR EXTRA OR AD- DITIONAL OR REDUNDANT OR SECOND? OR 2ND OR TWO) (3W) SIGNATURE? ?
S5	33	S1 AND S2
S6	19	RD (unique items)
S7	11	S1 AND S3
S8	7	RD (unique items)
S9	330	S1 AND S4
S10	24	S9 AND HASH???
S11	17	RD (unique items)
S12	16	S11 NOT (S6 OR S8)
S13	403	MULTISIGNATURE? ? OR MULTI() SIGNATURE? ?
S14	151	S1 AND S13
S15	28	S14 AND HASH???
S16	21	RD (unique items)
S17	19	S16 NOT (S6 OR S8 OR S12)
S18	264	("R2" OR R(1W) (SUP OR SUPP) (1W) (2 OR TWO)) (1W) ("S2" OR S(1- W) (SUP OR SUPP) (1W) (2 OR TWO))
S19	0	S1 AND S18
S20	0	S13 AND S18
S21	1	HASH??? AND S18
S22	33	("R1" OR R(1W) (SUP OR SUPP) (1W) (1 OR ONE)) (1W) ("S2" OR S(1- W) (SUP OR SUPP) (1W) (2 OR TWO))
S23	0	(S1 OR HASH???) AND S22

17/5/2 (Item 2 from file: 8)
DIALOG(R) File 8: Ei Compendex(R)
(c) 2004 Elsevier Eng. Info. Inc. All rts. reserv.

06395053 E.I. No: EIP03227484819

Title: Cryptanalysis of Shieh-Lin-Yang-Sun signature scheme

Author: Hwang, Shin-Jia; Li, En-Ti

Corporate Source: Dept. of Comp. Sci. and Info. Eng. Tamkang University,
Tamsui Taipei Hsien Taipei Hsien 251, Taiwan

Source: IEEE Communications Letters v 7 n 4 April 2003. p 195-196

Publication Year: 2003

CODEN: ICLEF6 ISSN: 1089-7798

Language: English

Document Type: JA; (Journal Article) Treatment: A; (Applications); T;
(Theoretical)

Journal Announcement: 0306W1

Abstract: Due to the special requirements of the mobile code system, in 2000, Shieh et al. proposed some **multisignature** schemes based on a new **digital signature** scheme with message recovery. One major characteristic of these schemes is to avoid using one-way **hash** functions and message redundancy schemes. However, this causes some security flaw. An attack is proposed to show that the underlying signature scheme is not secure. To overcome the attack, the message redundancy schemes may be still used. 13 Refs.

Descriptors: *Network protocols; Electronic document identification systems; Cryptography; Codes (symbols); Functions; Redundancy; Security of data

File 348:EUROPEAN PATENTS 1978-2004/Aug W02

(c) 2004 European Patent Office

File 349:PCT FULLTEXT 1979-2002/UB=20040812,UT=20040805

(c) 2004 WIPO/Univention

Set	Items	Description
S1	50362	(ELECTRONIC? OR DIGITAL?)(2N)(SIGNATURE? ? OR SIGN? ? OR SIGNED OR SIGNING) OR DSA
S2	1085	(WITHOUT OR NO OR "NOT" OR T)(5W)HASH??? OR HASHLESS OR UNHASHED
S3	11358	(SIGN OR SIGNS OR SIGNED OR SIGNING)(5W)(TWICE OR (TWO OR - 2ND OR SECOND OR ANOTHER OR EXTRA OR ADDITIONAL)(1W)TIME? ? OR MORE() (THEN OR THAN) OR AGAIN OR ONCE()MORE)
S4	2585	(MULTI OR MULTIPLE OR MULTIPLICITY OR SEVERAL OR MORE() (THEN OR THAN)()ONE OR MANY OR PLURAL? OR DUAL? OR ANOTHER OR EXTRA OR ADDITIONAL OR REDUNDANT OR SECOND? OR 2ND OR TWO)(3W)(SIGNATURE? ? OR SIGNING? ?)
S5	99	S1(50N)S2
S6	703	S1(50N)S3
S7	608	S1(50N)S4
S8	11	S1(50N)S2(50N)S3:S4
S9	15	S5/AB,CM
S10	134	S6/AB,CM
S11	180	S7/AB,CM
S12	23	S8:S9
S13	751	("R2" OR R(1W)(SUP OR SUPP)(1W)(2 OR TWO))(1W)("S2" OR S(1-W)(SUP OR SUPP)(1W)(2 OR TWO))
S14	245	("R1" OR R(1W)(SUP OR SUPP)(1W)(1 OR ONE))(1W)("S2" OR S(1-W)(SUP OR SUPP)(1W)(2 OR TWO))
S15	5	S1(100N)S13:S14
S16	27	S12 OR S15
S17	13	S16 AND AC=US/PR
S18	11	S17 AND AY=(1970:2000)/PR
S19	7	S16 AND PY=1970:2000
S20	15	S18:S19

File 347:JAPIO Nov 1976-2004/Apr(Updated 040802)

(c) 2004 JPO & JAPIO

File 350:Derwent WPIX 1963-2004/UD,UM &UP=200452

(c) 2004 Thomson Derwent

Set	Items	Description
S1	3907	(ELECTRONIC? OR DIGITAL?)(2N)(SIGNATURE? ? OR SIGN? ? OR S- IGNED OR SIGNING) OR DSA
S2	86	(WITHOUT OR NO OR "NOT" OR T)(5W)HASH??? OR HASHLESS OR UN- HASHED
S3	12227	SIGN??? (5W)(TWICE OR (TWO OR 2ND OR SECOND OR ANOTHER OR E- XTRA OR ADDITIONAL)(1W)TIME? ? OR MORE() (THEN OR THAN) OR AGA- IN OR ONCE()MORE)
S4	676	(MULTI OR MULTIPLE OR MULTIPLICITY OR SEVERAL OR MORE() (TH- EN OR THAN)()ONE OR MANY OR PLURAL? OR DUAL? OR ANOTHER OR EX- TRA OR ADDITIONAL OR REDUNDANT OR SECOND? OR 2ND OR TWO)(3W)S- IGNATURE? ?
S5	6	S1 AND S2
S6	6	S1 AND S3
S7	161	S1 AND S4
S8	12	S7 AND HASH???
S9	154	("R2" OR R(1W)(SUP OR SUPP)(1W)(2 OR TWO))(1W)("S2" OR S(1- W)(SUP OR SUPP)(1W)(2 OR TWO))
S10	75	("R1" OR R(1W)(SUP OR SUPP)(1W)(1 OR ONE))(1W)("S2" OR S(1- W)(SUP OR SUPP)(1W)(2 OR TWO))
S11	1	S1 AND S9:S10
S12	23	S5:S6 OR S8 OR S11

Abstract (Basic): WO 9737461 A

The inventive method signs a message (coin) into a **digital signature** of the sender, the signature being generated using public and sender secret generators, a sender private key, and other publicly known values. The message is then transmitted over e.g. in Internet, to the receiver.

The message to be signed incorporates a first predetermined function [f(x)] of the sender's public signature generator (48). Thus a receiver may verify the incorporation of such a proper first value. If the same message is **signed /transmitted more than** once, the sender's private key may be derived, from the plural signed messages using a relationship between the public/private signature generators.

USE/ADVANTAGE - Affordable, low-cost, off-line, micro-cash transmission system for purchasing information over Internet, with purchaser anonymity, not involving on-line Bank for payment, without using tamper-resistant devices, or purchaser/merchant interactive communication, and preferable to sending personal credit-card number (even encrypted) over network.

Dwg.4/6

Title Terms: MESSAGE; TRANSMISSION; NETWORK; CASH; PURCHASE; TRANSMIT; MESSAGE; BEARING; SEND; DIGITAL; SIGNATURE; FUNCTION; MESSAGE; PUBLIC; SEND; SECRET; GENERATOR; SEND; PRIVATE; KEY

Derwent Class: T01; T05; W01

International Patent Class (Main): H04L-009/00; H04L-009/32

International Patent Class (Additional): H04L-009/30

File Segment: EPI

12/5/19 (Item 12 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

011011100 **Image available**

WPI Acc No: 1996-508050/199651

XRFX Acc No: N96-428080

Zero-knowledge public key digital signature generation method - developing first and second signature hash code parameters reversibly transformed by third hash code parameter and dependent on message sent by signatory

Patent Assignee: FRANCE TELECOM (ETFR); LA POSTE (ETFR)

Inventor: GIRAULT M

Number of Countries: 003 Number of Patents: 004

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
EP 743775	A1	19961120	EP 96480053	A	19960430	199651 B
FR 2734435	A1	19961122	FR 956259	A	19950517	199703
EP 743775	B1	19980114				199807
DE 69600143	E	19980219	DE 600143	A	19960430	199813
			EP 96480053	A	19960430	

Priority Applications (No Type Date): FR 956259 A 19950517

Cited Patents: 2.Jnl.Ref

Patent Details:

Patent No Kind Lan Pg Main IPC Filing Notes

EP 743775 A1 F 18 H04L-009/32

Designated States (Regional): DE GB

EP 743775 B1 F 20 H04L-009/32

Designated States (Regional): DE GB

DE 69600143 E H04L-009/32 Based on patent EP 743775

FR 2734435 A1 H04L-009/30

Abstract (Basic): EP 743775 A

The method involves generating a first parameter (e) which is a **hash** code, f(c,M), and is produced by a one-way **hash** function, receiving an initial value (c) of a random value (r) and a signed message (M). A second parameter (y) is determined from the first

parameter (e), a secret key (s) and the random value. The third parameter is a **hash** code, g(M), produced by a second one-way **hash** code receiving as input the signed message.

A reversible transformation stage (35) combines the first and **second signature** parameters with first (g1) and second (g2) fractions of the third parameter or with the entire third parameter. The **hash** functions (f,g) of the first and second parameters may be identical.

USE/ADVANTAGE - E.g. computers, facsimile transmission, telephones, banking, smart cards. Collision resistant **hash** function and increased signature length not required. Simple without reducing data security.

Dwg.3/4

Title Terms: ZERO; PUBLIC; KEY; DIGITAL; SIGNATURE; GENERATE; METHOD; DEVELOP; FIRST; SECOND; SIGNATURE; **HASH** ; CODE; PARAMETER; REVERSE; TRANSFORM; THIRD; **HASH** ; CODE; PARAMETER; DEPEND; MESSAGE; SEND

Derwent Class: T01; T04; T05; W01; W02

International Patent Class (Main): H04L-009/30; H04L-009/32

File Segment: EPI

12/5/20 (Item 13 from file: 350)

DIALOG(R) File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

010818472 **Image available**

WPI Acc No: 1996-315425/199632

XRPX Acc No: N96-265583

Digital signature system for electronic document in computer network environment - has second computer which transmits error information to first computer if signature key is judged to be incorrect

Patent Assignee: NEC CORP (NIDE)

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
JP 8139717	A	19960531	JP 94272229	A	19941107	199632 B

Priority Applications (No Type Date): JP 94272229 A 19941107

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
JP 8139717	A	7	H04L-009/00	

Abstract (Basic): JP 8139717 A

The system uses a first and second computer which are connected in a network. The document for signature, user ID and the signature key are input to the first computer. A **hashing** part (14) is used to **hash** the document in the first computer. The user ID, signature key and the **hash** value are transmitted to the second computer.

The correctness of the signature key is judged by a judgment part. If the judgment result is correct, then, the **second** computer generates **digital signature**. This **digital signature** is fed to the first computer. If the signature key is incorrect, then the error information is transmitted to the first computer from the second computer.

ADVANTAGE - Performs **digital signature** efficiency.

Dwg.1/3

Title Terms: DIGITAL; SIGNATURE; SYSTEM; ELECTRONIC; DOCUMENT; COMPUTER; NETWORK; ENVIRONMENT; SECOND; COMPUTER; TRANSMIT; ERROR; INFORMATION; FIRST; COMPUTER; SIGNATURE; KEY; JUDGEMENT; INCORRECT

Derwent Class: P85; T01; W01

International Patent Class (Main): H04L-009/00

International Patent Class (Additional): G09C-001/00; H04L-009/10; H04L-009/12

File Segment: EPI; EngPI

12/5/21 (Item 14 from file: 350)

DIALOG(R) File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

File 275:Gale Group Computer DB(TM) 1983-2004/Aug 17
 (c) 2004 The Gale Group
 File 621:Gale Group New Prod.Annou.(R) 1985-2004/Aug 17
 (c) 2004 The Gale Group
 File 636:Gale Group Newsletter DB(TM) 1987-2004/Aug 17
 (c) 2004 The Gale Group
 File 16:Gale Group PROMT(R) 1990-2004/Aug 17
 (c) 2004 The Gale Group
 File 160:Gale Group PROMT(R) 1972-1989
 (c) 1999 The Gale Group
 File 148:Gale Group Trade & Industry DB 1976-2004/Aug 17
 (c)2004 The Gale Group
 File 624:McGraw-Hill Publications 1985-2004/Aug 16
 (c) 2004 McGraw-Hill Co. Inc
 File 15:ABI/Inform(R) 1971-2004/Aug 16
 (c) 2004 ProQuest Info&Learning
 File 647:CMP Computer Fulltext 1988-2004/Aug W2
 (c) 2004 CMP Media, LLC
 File 674:Computer News Fulltext 1989-2004/Jul W4
 (c) 2004 IDG Communications
 File 696:DIALOG Telecom. Newsletters 1995-2004/Aug 16
 (c) 2004 The Dialog Corp.
 File 369:New Scientist 1994-2004/Aug W2
 (c) 2004 Reed Business Information Ltd.

Set	Items	Description
S1	65545	(ELECTRONIC? OR DIGITAL?) (2N) (SIGNATURE? ? OR SIGN? ? OR SIGNED OR SIGNING) OR DSA
S2	756	(WITHOUT OR NO OR "NOT" OR T) (5W) HASH??? OR HASHLESS OR UNHASHED
S3	18532	(SIGN OR SIGNS OR SIGNED OR SIGNING) (5W) (TWICE OR (TWO OR - 2ND OR SECOND OR ANOTHER OR EXTRA OR ADDITIONAL) (1W) TIME? ? OR MORE() (THEN OR THAN) OR AGAIN OR ONCE() MORE)
S4	10970	(MULTI OR MULTIPLE OR MULTIPLICITY OR SEVERAL OR MORE() (THEN OR THAN) () ONE OR MANY OR PLURAL? OR DUAL? OR ANOTHER OR EXTRA OR ADDITIONAL OR REDUNDANT OR SECOND? OR 2ND OR TWO) (3W) (- SIGNATURE? ? OR SIGNING? ?)
S5	17	S1(50N)S2
S6	124	S1(50N)S3
S7	809	S1(50N)S4
S8	141	S5:S6
S9	84	RD (unique items)
S10	42	S9 NOT PD>20000328
S11	13	("R1" OR R(1W) (SUP OR SUPP) (1W) (1 OR ONE)) (1W) ("S2" OR S(1-W) (SUP OR SUPP) (1W) (2 OR TWO))
S12	138	("R2" OR R(1W) (SUP OR SUPP) (1W) (2 OR TWO)) (1W) ("S2" OR S(1-W) (SUP OR SUPP) (1W) (2 OR TWO))
S13	0	S1(100N)S11:S12
S14	42	S10